Amber L. Schubert (No. 278696)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, California 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
aschubert@sjk.law

Counsel for Plaintiff Jill Strelzin and her minor children

UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

PLAINTIFF JILL STRELZIN, on behalf of J.S., a minor, and R.S., a minor, and all others similarly situated, *Plaintiff*, v. POWERSCHOOL GROUP, LLC, and POWERSCHOOL HOLDINGS, INC., *Defendant*.	No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Jill Strelzin, on behalf of J.S., a minor, and R.S., a minor ("Plaintiff"), by her undersigned counsel, files this Class Action Complaint individually on their behalf and on behalf a class of all similarly situated persons against Powerschool Group, LLC and Powerschool Holdings, Inc. (collectively, "Defendant" or "PowerSchool"). Plaintiff bases the following allegations on personal knowledge, due investigation of counsel, and, where indicated, on information and belief, and states the following:

NATURE OF THE ACTION

1. PowerSchool is a cloud-based software solutions provider for K-12 schools and districts that reportedly supports over 17,00 customers (ie, schools and school districts) worldwide. Powerschool reportedly serves more than 50 million students in the United States, and over 75% of students in North America. PowerSchool offers a panoply of services to help its customer schools' operation, including but not limited to providing platforms to manage enrollment, communication, attendance, staff management, learning systems, analytics, finance, and grades.

2. As a major provider of cloud-based software services to the students across the United States, PowerSchool understood it had the duty and responsibility to protect students' information that it collected, stored, and maintained, expressly advertising to schools and students that:

> We seek to protect our customers' personal data from unauthorized access, use, modification, disclosure, loss, or theft by leveraging various reasonable security measures and methods to secure our customers' personal data throughout its processing lifecycle with PowerSchool applications. Our overall aim is to ensure the confidentiality, integrity, and availability of our customers' personal data by leveraging technical, organizational, and where appropriate, physical security methods. Security protection at PowerSchool is a cross-functional activity that intersects our workforce duties, and we have relevant security and privacy policies to drive expectations from the workforce. [1]

3. On January 7, 2025, Defendant began announcing to schools across the country that an unauthorized threat actor had accessed personal employee and student information from customers worldwide using the PowerSchool Student Information System ("PowerSchool SIS"). The threat actor accessed and downloaded millions of records from schools worldwide between December 19 and December 24, 2024 (the "Data Breach").

[1] PowerSchool's Privacy Principles, PowerSchool (updated October 1, 2024) https://www.powerschool.com/privacy/ (last accessed January 10, 2025).

4. The highly sensitive personally identifying information ("PII") released to the threat actor included information from students and employees (ie, teachers) at schools using PowerSchool's services, including, *inter alia*:

Students

- Student names and ID numbers
- Parent/guardian contact information
- Dates of enrollment and withdrawal reasons
- Limited medical alert information (e.g., allergies, life-threatening conditions)
- IEP and 504 status
- Social Security numbers
- Free and reduced lunch status
- Grades, grade point averages
- Medical information
- Bus stops
- Passwords
- Notes
- Alerts

Employees

- Employee names and ID numbers
- Department
- Employee type
- School email address
- School phone number

- Social Security Number
- Passwords
- Addresses

5. Worse yet, this much of this data relates to minors under the age of eighteen, further heightening the high sensitivity of this information.

6. In order to obtain Defendant's services, individuals must entrust PowerSchool with sensitive, private information. Defendant requires this information in order to perform its regular business activities.

7. As a direct and proximate result of Defendant's inadequate data security measures, and its breach of its duty to handle PII with reasonable care, Plaintiff's minor children's and Class Members' PII have been accessed by hackers and exposed to an untold number of unauthorized individuals.

8. Plaintiff's minor children and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff's minor children and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. Plaintiff, her minor children, and the Class, as defined herein, bring claims for negligence, negligence *per se*, breach of an implied third-party contract, unjust enrichment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

11. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

PARTIES

13. Plaintiff Jill Strelzin is the mother and legal guardian of J.S. and R.S., who at all relevant times, were residents of the State of Illinois. J.S. and R.S. attend high school in Glenbrook High School District 225 ("School District") in Cook County, Illinois. J.S. and R.S.' high school uses PowerSchool SIS to conduct its operations. On January 8, 2025, Plaintiff Strelzin received an email notice from the School District advising her that portions of over *fifty thousand* current and former student records had been accessed in the Data Breach, in addition to portions of over 5,000 employee records. Upon information and belief, J.S.' and R.S.' student records were accessed in the Data Breach.

14. Since the unauthorized access of information involved in the Data Breach, Plaintiff and her minor children have suffered emotional distress as a result of their PII being accessed and exposed to unauthorized third parties.

15. As a result of the Data Breach, Plaintiff's minor children will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

16. PowerSchool Group, LLC is a corporation organized under the laws of Delaware and maintains its headquarters and principal place of business at 150 Parkshore Drive, Folsom, CA 95630.

17. PowerSchool Holdings, Inc. is a corporation organized under the laws of Delaware and maintains its headquarters and principal place of business at 150 Parkshore Drive, Folsom, CA 95630.

FACTUAL BACKGROUND

A. Defendant Collected Plaintiff's Minor Children's and Class Members' PII as a Necessary Part of Its Routine Business Dealings with Them.

18. PowerSchool is reportedly the largest provider of cloud-based education software for K-12 education. PowerSchool touts its powerful PowerSchool SIS allowing schools the ability to "Manage School Operations from Anywhere." Specifically, Defendant advertises PowerSchool SIS as collecting and organizing all student information in a secure, cloud based platform that can be customized to power many aspects of school operations, including but not limited to verifying student address and boundaries, advanced grading calculations, attendance, course creation, assignments, history, and recommendations, enrollment, data integrity and security, fees, health & immunizations, honor roll and class rank, parent and student portals, report cards, and integrated analytics.[2]

[2] *See Explore All PowerSchool SIS Has to Offer*, PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis/features/ (last accessed January 10, 2025).

19. As a condition of receiving PowerSchool's PowerSchool SIS services, customers must provide it with sensitive student and teacher PII, set forth more fully *supra*, which may include but is not limited to students' names, social security numbers, addresses, school and grade information, medical information, and bus stop information.

20. PowerSchool derives substantial benefit from this information because, but for the collection of students' and teachers' PII, Defendant would be unable to perform any of its school data management services.

21. PowerSchool acknowledges the vast amounts of PII with which it is entrusted and admits the "processing of personal data" is central to its operations.[3] In addition to its promises set forth *supra*, PowerSchool promises that "we use state-of-the-art, and appropriate physical, technical, and administrative security measures to protect the personal data that we process."[4]

22. PowerSchool goes on to tout its "Commitment to Protecting Your Data", stating:

> **How is your personal information protected?** PowerSchool employs a variety of physical, administrative, and technological safeguards designed to protect your data against loss, misuse, and unauthorized access or disclosure. We strive to continuously maintain reasonable physical, administrative, and technical security measures. Our security measures consider the type and sensitivity of the data being collected, used, and stored, and the current state of technology and threats to data. PowerSchool independently verifies its security management system to the internationally recognized standard for security management and holds ISO 27001 and SOC2 certifications. PowerSchool also endeavors to align its privacy and security operations to best practices and relevant international regulations.[5]

[3] *PowerSchool's Privacy Principles*, PowerSchool, https://www.powerschool.com/privacy/ (last accessed January 10, 2025).
[4] *Frequently Asked Questions*, PowerSchool, https://www.powerschool.com/privacy/ (last accessed January 10, 2025).
[5] *Global Privacy Statement*, PowerSchool (last updated October 1, 2024), https://www.powerschool.com/privacy/ (last accessed January 10, 2025).

23. Plaintiff, her minor children, and Class Members directly or indirectly entrusted PowerSchool with their sensitive and confidential PII, as did their schools who contracted with Defendant, and therefore reasonably expected that Defendant would safeguard their highly sensitive PII and keep it confidential.

24. By obtaining, collecting, and storing Plaintiff's minor children's and Class Members' PII, PowerSchool assumed equitable and legal duties to safeguard and keep confidential Plaintiff's minor children's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

25. Despite these duties, PowerSchool failed to implement reasonable data security measures to protect Plaintiff's minor children's and Class Members' PII and ultimately allowed nefarious third-party hackers to breach its computer systems, compromising Plaintiff's minor children's and Class Members' PII stored therein.

B. PowerSchool Knew the Risks of Storing Valuable PII and the Foreseeable Risk of Harm to Victims.

26. PowerSchool was well aware that the PII it acquires is highly sensitive and of significant value to those who would use it for wrongful purposes.

27. PowerSchool also knew that a breach of its computer systems, and release of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private information.

28. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

29. PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft and medical

and financial fraud.[6] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

30. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available. Indeed, the information compromised during the Data Breach may have already been released on the internet.

31. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2023, there were 3,205 data compromises affecting 353 million individuals, which set a record high number of data compromises in the U.S. in a single year, representing a 72% increase from the previous all-time high number of comprises set in 2021.[7]

32. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2019, approximately 650,000 people reported identity fraud compared to over a million people in 2023, representing an increase of approximately 19%.[8]

[6] *What To Know About Identity Theft*, Fed. Trade Comm'n Consumer Advice (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed January 10, 2025).

[7] *Facts + Statistics; Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last accessed January 10, 2025).

[8] *Id*.

33. The breath of data compromised makes the information particularly vulnerable to thieves and leaves PowerSchool's customers especially vulnerable to fraud and other risks.

34. The ramifications of PowerSchool's failure to keep Plaintiff's minor children's and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

35. Further, a data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[9]

36. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

37. Moreover, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, information such as social

[9] Erika Harrell, Bureau of Just. Stat., U.S. Dep't of Just., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed January 10, 2025).

security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies to update the person's accounts with those entities.

38. The Social Security Administration even warns that the process of replacing a social security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[10]

39. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

[10] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed January 10, 2025).

40. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[11]

41. In light of high-profile data breaches at other companies, PowerSchool knew or should have known that its computer systems would be targeted by cybercriminals.

42. Defendant also knew or should have known the importance of safeguarding the PII with which it was entrusted and of the foreseeable consequences if its data security systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach and release of its customers' PII from occurring.

C. Defendant Released Highly Sensitive PII to Hackers and Breached its Duty to Protect Customer PII.

43. On the afternoon of January 7, 2025, PowerSchool began sending notification of the Data Breach to impacted customers.[12]

44. Defendant's notice advised, in part, that it learned on December 28, 2024 of a cybersecurity incident involving unauthorized access to one of its customer support portals, PowerSource. The threat actor gained access to PowerSource using compromised credentials, which contains an access tool allowing PowerSchool engineers to access Customer SIS instances.[13]

[11] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, Forbes (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed January 10, 2025).
[12] *PowerSchool hack exposes student, teacher data from K-12 districts*, Bleeping Computer (January 7, 2025), https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/ (last accessed January 10, 2025).
[13] *Id*.

Using this tool, the attacker gained access to PowerSchool SIS and exported the PowerSchool SIS "Students" and "Teachers" database tables to a CVS file, which was then stolen.[14]

45. PowerSchool also confirmed that stolen data contains contact details such as names and addresses and may also include social security numbers, personally identifiable information, medication information, grades, and more.[15]

46. Impacted schools in turn provided notice to students and parents whose PII was impacted. For example, the School District sent notice to Plaintiff advising that portions of over 50,000 current and former students and over 5,000 employee records were accessed in the breach. *See* Exhibit A (Notice Letter). The Notice Letter also advised that, in total, the threat actor accessed and downloaded millions of records from schools worldwide between December 19 and December 24, 2024. *Id*. Impacted information included information such as:

Students

- Student names and ID numbers
- Parent/guardian contact information
- Dates of enrollment and withdrawal reasons
- Limited medical alert information (e.g., allergies, life-threatening conditions)
- IEP and 504 status
- A limited number of Social Security numbers that were collected between 2005 and 2017

Free and reduced lunch status

Employees

- Employee names and ID numbers

[14] *Id*.
[15] *Id*.

- Department
- Employee type
- School email address
- School phone number

Id.

47. Although many schools are still determining the extent of the breach, schools across the country are sending similar notice to impacted individuals. For example, several schools in Massachusetts use PowerSchool's software, and officials reported that student information, including addresses, grades, and health information, may have been compromised in the breach.[16] Boston cybersecurity experts have recommending parents freezing their child's credit and investing in identity theft protection.[17] Likewise, Kalamzoo Public Schools, in Michigan, sent notice to affected families that accessed information included names, addresses, grade levels, and demographics of students.[18] Rose Hills Schools in Kansas also gave notice that it was impacted by the breach and that access information may include names, addresses, phone numbers, student health information, and student grade information.[19] Randolph Public School District, located in Massachusetts, gave notice that downloaded information included student names, addresses, phone numbers, email addresses, ID numbers, birthdays, and some health information such as

[16] *Massachusetts school districts warn parents after PowerSchool data breach*, WCVB5, ABC (January 10, 2025), https://www.wcvb.com/article/massachusetts-school-districts-parents-powerschool-data-breach/63379956 (last accessed January 10, 2025).
[17] *Id*.
[18] *Kalamazoo, Paw Paw Schools among multiple districts impacted by PowerSchool data breach*, News Channel 3 (January 9, 2025), https://wwmt.com/news/arc/kalamazoo-paw-paw-schools-data-breach-powerschool-student-information-system-education-community-west-michigan (last accessed January 10, 2025).
[19] *PowerSchool Data Breach: What You Need to Know*, Rose Hill Schools USD 394 (January 8, 2025), https://www.usd394.com/article/1953590 (last accessed November 10, 2025).

allergies, and staff ID numbers, social security numbers, and dates of birth.[20] Similarly, public schools in Indianapolis, Indiana, reported that accessed information included student addresses, phone numbers, date of birth, grade in school, grade point average, and medical alert information (such as asthma, diabetes), parent/guardian addresses and phone numbers, and teacher/administrator directory information and the last four digits of their social security number.[21]

48. In sum, upon information and belief, as a result of Defendant's failure to implement adequate data security measures, Plaintiff's minor children's and Class Members' PII, was negligently released to unauthorized, malicious threat actors and is now at risk of dissemination and use by other unauthorized individuals or cybercrime groups.

D. Defendant Failed to Comply with FTC Guidelines.

49. PowerSchool is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

[20] *Cybersecurity Memorandum: PowerSchool Data Breach*, Randolph Public School District (January 9, 2025), https://www.randolph.k12.ma.us/news/1802130/cybersecurity-memorandum-powerschool-data-breach (last accessed January 10, 2025).

[21] *PowerSchool Cybersecurity Data Breach*, Indianapolis Public Schools (January 9, 2025), https://myips.org/blog/district/powerschool-cybersecurity-data-breach/ (last accessed January 9, 2025).

50. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[22]

51. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures, including:[23]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

[22] *Start with Security: A Guide for Business*, Fed. Trade Comm'n (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed January 10, 2025).

[23] *Protecting Personal Information: A Guide for Business*, U.S. FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed January 10, 2025).

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. Upon information and belief, PowerSchool failed to properly implement one or more of the basic data security practices described above. PowerSchool's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized release of Plaintiff's minor children's and Class Members' PII to a nefarious threat actor. Further, PowerSchool's failure to implement basic data security practices constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

54. PowerSchool was at all times fully aware of its obligations to protect the PII of consumers because of its business model of collecting and processing highly sensitive PII of minors. PowerSchool was also aware of the significant repercussions that would result from its failure to do so.

55. PowerSchool's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. Plaintiff's Minor Children and Members of the Class Have Suffered Concrete Injury.

56. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff, her minor children, and members of the Class, significant injuries and harm in several ways. Plaintiff, her minor children, and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

57. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff, her minor children, and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendant's conduct. Further, the value of Plaintiff's minor children's and Class Members' PII has been diminished by its exposure in the Data Breach.

58. As a result of Defendant's failures, Plaintiff's minor children and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII.

59. In 2021 alone, identity theft victims in the United States had financial losses totaling $16.4 billion.[24]

60. Besides the monetary damage sustained, consumers may also spend anywhere from one day to more than six months resolving identity theft issues.[25]

61. Ultimately, the time that victims spend monitoring and resolving identity theft issues takes an emotional toll. Approximately 80% of victims of identity theft experienced some type of emotional distress, and more than one-third of victims experienced moderate or severe emotional distress.[26]

62. Plaintiff, her minor children, and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

63. As a result of PowerSchool's failure to prevent the Data Breach, Plaintiff, her minor children, and Class Members have suffered and will continue to suffer injuries, including loss of

[24] Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021*, U.S. Dept. Just., Bureau Just. Stats. (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf (last accessed January 10, 2025).
[25] *Supra* note 35.
[26] *Id.*

time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their highly valuable PII; the imminent and certainly impending injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiff's minor children's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII with which it was entrusted.

F. Plaintiff's Minor Children and Members of the Class Are Now at an Increased Risk of Future Harms.

64. Data Breaches such as the one experienced by Plaintiff's minor children and Class Members are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

65. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[27] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiff, her minor children, and Class Members) must take after a Data Breach like PowerSchool's are both time-consuming and of only limited and short-term effectiveness.

[27] Government Accountability Off., "Data Breaches" (Mar. 2019) https://www.gao.gov/assets/gao-19-230.pdf (last accessed January 10, 2025).

66. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

67. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[29]

68. Theft of PII is also gravely serious as PII is a valuable property right.[30]

69. There may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the GAO, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

70. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

---

[28] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," Government Accountability Off. (June 2007), https://www.gao.gov/new.items/d07737.pdf ("2007 GAO Report") (last accessed April 4, 2024).

[29] *See* Identity Theft Victim Checklist, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last accessed January 10, 2025).

[30] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("SPI") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("SPI, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[31] *See* 2007 GAO Report, at 29.

71. Because the entirety of the stolen information has *already* been released on the dark web, every Class Member, including Plaintiff's minor children, is at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff's minor children and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

G. Plaintiff's and Her Minor Children's Experience.

72. Plaintiff Jill Strelzin is the mother and legal guardian of J.S. and R.S., who attends the School District in Cook County, Illinois. J.S. and R.S.'s high school uses PowerSchool SIS to conduct its operations. On January 8, 2025, Plaintiff Strelzin received the Notice Letter from the School District advising her that the School District was impacted by the breach and PII of its students was accessed. *See* Exhibit A. Specifically, the notice advised that portions of 53,740 current and former student records had been accessed in the Data Breach, in addition to portions of 5,195 employee records. Upon and information and belief, J.S.' and R.S.' student records were accessed in the Data Breach.

73. Additionally, the Notice Letter disclosed that student records were accessed including names and ID numbers, parent/guardian contact information, dates of enrollment and withdrawal reasons, medical alert information (allergies, life-threatening conditions), IEP and 504 status, social security numbers collected between 2005 and 2017, and free and reduced lunch status. Furthermore, the School District's employee records were accessed, including names and ID numbers, department, employee type, school email address, and school phone number.

74. Importantly, when providing Plaintiff's minor children's PII, Plaintiff and her minor children at all times expected the information to be kept confidential. Plaintiff and her minor children likewise expected any PII generated by the School District and provided to Defendant would be kept strictly confidential.

75. Since the Data Breach, Plaintiff and/or her minor children have spent numerous hours on behalf of her minor children taking action to mitigate the impact of the Data Breach, which included additional review and monitoring of her and her minor children's personal and financial accounts, endeavoring to implement additional security measures where appropriate, and researching credit card monitoring services. Plaintiff took these mitigation efforts and incurred this loss of time as a direct and proximate result of the Data Breach.

76. Knowing that a threat actor stole her minor children's PII has caused Plaintiff and her minor children anxiety. They are now very concerned about identity theft and impending privacy harms arising from the Data Breach. Plaintiff further has concerns of Defendant suffering future data breaches or otherwise releasing Plaintiff's PII in the future.

77. Plaintiff and her minor children have suffered actual injury from having their PII exposed as a result of the Data Breach, including, but not limited to: (a) allowing their PII to be disclosed to Defendant, which Plaintiff would not have allowed had Defendant disclosed that it lacked data security practices to safeguard its PII from theft; (b) damages to and diminution in value of Plaintiff's minor children's PII—a form of intangible property that Plaintiff and her minor children entrusted to PowerSchool; (c) loss of privacy; (d) lost time; and (e) imminent and impending injury arising from the increased risk of fraud and identity theft.

78. As a result of the Data Breach, Plaintiff's minor children will continue to be at a heightened risk for identity theft and attendant damages for years to come.

CLASS ALLEGATIONS

79. Plaintiff brings this case on behalf of J.S., a minor, and R.S., a minor and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose PII was compromised in the PowerSchool Data Breach (the "Class").

80. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

81. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

82. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. Defendant has not stated the number of individuals implicated in the Data Breach, but millions of student and employee documents were accessed in the Data Breach.

83. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the PII of Plaintiff's minor children and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's minor children's and Class Members' PII, and breached its duties thereby;

c. Whether Defendant obtained Plaintiff's minor children's and Class Members' PII;

d. Whether Defendant released Plaintiff's minor children's and Class members' PII without authorization;

e. When Defendant learned of the Data Breach;

f. Whether Defendant adequately and timely responded to the Data Breach;

g. Whether Defendant failed to maintain reasonable security systems and procedures, including those required by applicable security laws and regulations and those consistent with industry standards;

h. Whether Defendant remedied the vulnerabilities that permitted the Data Breach to occur;

i. Whether Plaintiff, her minor children, and Class Members are entitled to actual damages, statutory damages, and/or other equitable relief as a result of Defendant's wrongful conduct; and

j. Whether Plaintiff, her minor children, and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

84. **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. The claims of Plaintiff, her minor children, and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard their PII. Plaintiff, her minor children, and Class Members entrusted Defendant with their PII, and it was subsequently released to an unauthorized third party.

85. **Adequacy of Representation.** Plaintiff and her minor children are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members Plaintiff and her minor children seek to represent; Plaintiff and her minor children have retained counsel competent and experienced in complex class action litigation and data breach litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has

adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff, her minor children, and Plaintiff's counsel.

86. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

87. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff, her minor children, and each member of the Class. If Defendant breached its duty and released Plaintiff's minor children's and Class Members' PII, then Plaintiff's minor children and each Class member suffered damages by that conduct.

88. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On behalf of Plaintiff and the Class)

89. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

90. Defendant owed a duty under common law to Plaintiff's minor children and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

91. PowerSchool's duty to use reasonable care arose from several sources, including but not limited to those described below.

92. Defendant has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff's minor children and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By receiving, maintaining, and handling PII that is routinely targeted by criminals for unauthorized access, PowerSchool was obligated to act with reasonable care to protect against these foreseeable threats.

93. PowerSchool breached the duties owed to Plaintiff's minor children and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control

these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

94. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff's minor children and Class Members, the PII in its possession would not have been compromised.

95. As a direct and proximate result of Defendant's negligence, Plaintiff's minor children and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and

identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's minor children's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's minor children's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff's minor children and Class members.

96. As a direct and proximate result of Defendant's negligence, Plaintiff's minor children and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(Plaintiff on Behalf of the Class)

97. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

98. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of PowerSchool's duty.

99. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving the PII it entrusted from its customers.

100. Plaintiff's minor children and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

101. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

102. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act is intended to guard against.

103. As a direct and proximate result of Defendant's negligence, Plaintiff's minor children and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's minor children's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's minor children's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff's minor children and Class members.

104. As a direct and proximate result of Defendant's negligence, Plaintiff's minor children and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(Plaintiff on Behalf of the Class)

105. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

106. Plaintiff brings this claim on behalf of her minor children and on behalf of the Class.

107. Prior to storing and processing data with Defendant's services, each of Defendant's customers, including the School District, entered into a contract with Defendant, under which, upon information and belief, Defendant agreed to take reasonable steps to protect data stored in their systems, including Plaintiff's minor children's and Class Members' PII, and to comply with their statutory and common law duties to protect Plaintiff's minor children's and Class Members' PII.

108. Upon information and belief, each such contract Defendant entered into with its clients was substantially similar with respect to Defendant's duty to safeguard data, including Plaintiff's minor children's and Class Members' PII. Further, each such contract was made for Plaintiff's minor children's and Class Members' direct benefit, and for each such contract, and Defendant's secure housing of PII was a material obligation that was specifically bargained for.

109. As set forth above and throughout, Defendant failed to fulfill its obligations to safeguard this data, including Plaintiff's minor children's and Class Members' PII. Defendant at all times knew that any such breach of this duty would proximately cause the following harm to Plaintiff's minor children and Class Members.

110. Upon information and belief, Defendant's clients would not have provided their data to Defendant had they known that Defendant would not safeguard it, as promised.

111. The losses and damages Plaintiff's minor children and Class Members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant

would safeguard Plaintiff's minor children's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's minor children's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff's minor children and Class Members.

112. As a direct and proximate result of Defendant's breach of these contract, Plaintiff's minor children and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiff on Behalf of the Class)

113. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

114. Plaintiff brings this claim on behalf of her minor children and on behalf of the Class in the alternative to Plaintiff's Breach of Third-Party Beneficiary Contract claim.

115. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's minor children's and Class Members' PII, which cost savings increased the profitability of its services.

116. Upon information and belief, instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff's minor children and Class Members by utilizing cheaper, ineffective security measures. Plaintiff's minor children and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

117. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff's minor children and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

118. Defendant acquired the monetary benefit, PII, through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

119. Had Plaintiff's, her minor children, and Class Members known that Defendant had not secured its PII, they would not have agreed to provide PII to Defendant. Plaintiff's minor children and Class Members have no adequate remedy at law.

120. As a direct and proximate result of Defendant's conduct, Plaintiff's minor children and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's minor children's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's minor children's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff's minor children and Class Members.

121. Plaintiff's minor children and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

122. Plaintiff's minor children and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

123. Moreover, Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff's minor children and Class Members, proceeds that it unjustly received from them.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiff on Behalf of the Class)

124. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

125. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

126. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's minor children's and Class Members' PII and whether PowerSchool is currently maintaining data security measures adequate to protect Plaintiff's minor children and Class Members from further data breaches that compromise their PII. Plaintiff alleges that PowerSchool's data security measures remain inadequate. Furthermore, Plaintiff's minor children

continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

127. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed a legal duty to secure customers PII under the common law and Section 5 of the FTC Act; and

b. Defendant breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

128. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect customers' PII.

129. If an injunction is not issued, Plaintiff's minor children and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at PowerSchool. The risk of another such breach is real, immediate, and substantial. If another breach at PowerSchool occurs, Plaintiff's minor children will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

130. The hardship to Plaintiff, her minor children, and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff's minor children will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

131. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at PowerSchool, thus eliminating the additional injuries that would result to Plaintiff, her minor children, Class Members, and customers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of her minor children and all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff, her minor children, and the Class on all counts asserted herein;

c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: January 10, 2025

Respectfully submitted,

/s/ Amber L. Schubert
Amber L. Schubert
SCHUBERT JONCKHEER & KOLBE
2011 Union St., Suite 200
San Francisco, CA 94128
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
E-mail: aschubert@sjk.law

Jonathan M. Jagher*
FREED KANNER LONDON & MILLEN LLC
923 Fayette Street
Conshohocken, PA 19428
610.234.6486
jjagher@fklmlaw.com

Nicholas R. Lange*
FREED KANNER LONDON & MILLEN LLC
100 Tri-State International Drive, Suite 128
Lincolnshire, IL 60629
224.632.4500
nlange@fklmlaw.com

**pro hac vice forthcoming*